修 士 学 位 論 文

論文題名
テータ関数に基づく Kummer 曲面上の擬加法に関する等分多項式

指導教授　内田　幸寛　准教授

平成 30 年 1 月 10 日　提出

首都大学東京　大学院
理工学研究科　数理情報科学専攻
学修番号 16878310

氏名　小澤 英泰

目次

1 概要

楕円曲線暗号は IC カードや仮想通貨を支えるブロックチェーンに使用されている. 楕円曲線暗号の一般化である超楕円曲線暗号は 1989 年に Koblitz により提案された. 安全な種数 2 の超楕円曲線暗号を構成するためには, ヤコビアンの位数がヤコビアンの位数の最大の素因子と同程度である必要がある. そのため, ヤコビアンの位数計算は重要である. 位数計算法の 1 つとして, Schoof のアルゴリズムを拡張したもの [3] がある. Gaudry [8] は, テータ関数に基づく Kummer 曲面上の擬加法を与え, Kummer 曲面と種数 2 の超楕円曲線のヤコビアンとの関係を与えた. これより, Kummer 曲面上の等分多項式を用いることで, ヤコビアンの位数を求めることができる. 本論文では, テータ関数に基づく Kummer 曲面上の擬加法に関する等分多項式 μ_m の存在を示し, 実際に構成した.

最初に, 本論文の内容を説明するために, 定義を与える.

$\mathbf{a}, \mathbf{b} \in \mathbb{Q}^2,\ \mathbf{z} \in \mathbb{C}^2$ とする. $\mathcal{H}_2 = \{A \in M(2, \mathbb{C}) \mid A = {}^tA,\ \mathrm{Im}A > 0\}$ に対して, $\mathbf{\Omega} \in \mathcal{H}_2$ とする. 指標付きテータ関数を以下で定義する.

$$\vartheta[\mathbf{a}; \mathbf{b}](\mathbf{z}, \mathbf{\Omega}) = \sum_{\mathbf{n} \in \mathbb{Z}^2} \exp(\pi i {}^t(\mathbf{n} + \mathbf{a})\mathbf{\Omega}(\mathbf{n} + \mathbf{a}) + 2\pi i {}^t(\mathbf{n} + \mathbf{a}) \cdot (\mathbf{z} + \mathbf{b})).$$

また, 基本テータ関数を以下で定義する.

$$\vartheta_1(\mathbf{z}) = \vartheta[(0,0); (0,0)](\mathbf{z}, \mathbf{\Omega}),\ \vartheta_2(\mathbf{z}) = \vartheta\Big[(0,0); \Big(\frac{1}{2}, \frac{1}{2}\Big)\Big](\mathbf{z}, \mathbf{\Omega}),$$
$$\vartheta_3(\mathbf{z}) = \vartheta\Big[(0,0); \Big(\frac{1}{2}, 0\Big)\Big](\mathbf{z}, \mathbf{\Omega}),\ \vartheta_4(\mathbf{z}) = \vartheta\Big[(0,0); \Big(0, \frac{1}{2}\Big)\Big](\mathbf{z}, \mathbf{\Omega}).$$

$\vartheta_1(\mathbf{z}), ..., \vartheta_4(\mathbf{z})$ は偶関数である. さらに, $\mathbf{z} = \mathbf{0}$ での指標付きテータ関数の値をテータ定数と呼び, 4 個のテータ定数を定義する.

$$a = \vartheta_1(\mathbf{0}),\ b = \vartheta_2(\mathbf{0}),\ c = \vartheta_3(\mathbf{0}),\ d = \vartheta_4(\mathbf{0}).$$

$\mathbf{\Omega}$ に付随する Kummer 曲面 $\mathcal{K}$ を

$$\kappa \colon \mathbf{z} \mapsto (\vartheta_1(2\mathbf{z}) \colon \vartheta_2(2\mathbf{z}) \colon \vartheta_3(2\mathbf{z}) \colon \vartheta_4(2\mathbf{z}))$$

により定まる, Abel 多様体 $J = \mathbb{C}^2/(\mathbb{Z}^2 + \mathbf{\Omega}\mathbb{Z}^2)$ から $\mathbb{P}^3(\mathbb{C})$ への写像 κ の像と定義する.

ϑ_i は偶関数より κ は準同型写像ではない. しかし, $\mathcal{K}$ 上の点に対して, 2 倍と擬加法を定められる. つまり, 未知の $\mathbf{z}, \mathbf{z}' \in J$ に対して, $\kappa(\mathbf{z}), \kappa(\mathbf{z}'), \kappa(\mathbf{z} - \mathbf{z}')$ が既知であれば, $\kappa(2\mathbf{z}), \kappa(\mathbf{z} + \mathbf{z}')$ を計算できる. $\mathcal{K}$ 上の擬加法に関する単位元は $O = (a, b, c, d)$ である.

$P \in J$ に対して, $\mathcal{K}$ 上の点を $\kappa(P) = (\xi_1(P) \colon \xi_2(P) \colon \xi_3(P) \colon \xi_4(P)) = (\xi_1 \colon \xi_2 \colon \xi_3 \colon \xi_4)$ と書く. O' を J の単位元とする. このとき, $\kappa(O') = O$ となる. $\mathcal{K}$ の射影方程式は以下で与えられる.

$$L \colon \xi_1^4 + \xi_2^4 + \xi_3^4 + \xi_4^4 + 2E\xi_1\xi_2\xi_3\xi_4 - F(\xi_1^2\xi_4^2 + \xi_2^2\xi_3^2) - G(\xi_1^2\xi_3^2 + \xi_2^2\xi_4^2) - H(\xi_1^2\xi_2^2 + \xi_3^2\xi_4^2) = 0.$$

但し, E, F, G, H は a, b, c, d の有理式である.

次に, 主結果について述べる.

Gaudry [8] によれば適切な条件の下で, 標数 0 から正標数に還元でき, 有限体 $\mathbb{F}_q$ 上でも 2 倍と擬加法が成り立つ.

k を標数が 0 の体または, 有限体とする. $a, b, c, d \in k^{\times}$ とし, k の代数閉包を $\bar{k}$ で表す. 次の性質を満たす多項式 $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$, B_i を作れる. 任意の $P, Q \in J(\bar{k})$ に対して, 定数 $c' \in \bar{k}^{\times}$ が存在し, $i = 1, 2, 3, 4$ に対して,

$$\kappa([2]P) = \delta(\kappa(P)),$$
$$\xi_i(P+Q)\xi_i(P-Q) = c' \cdot B_i(\kappa(P), \kappa(Q)).$$

この多項式を用いて, m 倍写像を表す多項式を得た.

主定理 1. 任意の $m \in \mathbb{Z}_{\geq 0}, i = 1, 2, 3, 4$ に対して, 以下を満たす斉次多項式 $\mu_{m,i} \in k[\xi_1, ..., \xi_4]/\langle L \rangle$ が存在する.

$$\mu_{0,1} = a, \mu_{0,2} = b, \mu_{0,3} = c, \mu_{0,4} = d,$$
$$\mu_{1,i} = \xi_i,$$
$$\mu_{2m,i} = \delta_i(\mu_m) \quad (m \geq 1),$$
$$\mu_{2m+1,i}\xi_i = B_i(\mu_{m+1}, \mu_m) \quad (m \geq 1).$$

但し, $\mu_m = (\mu_{m,1}, \mu_{m,2}, \mu_{m,3}, \mu_{m,4})$ である. また, 任意の $P \in J(\bar{k})$ に対して,

$$\kappa([m]P) = (\mu_{m,1}(\kappa(P)) : \mu_{m,2}(\kappa(P)) : \mu_{m,3}(\kappa(P)) : \mu_{m,4}(\kappa(P))).$$

主定理 1 は [12] と同様であるが, 違いは Kummer 曲面の定義の方法である.[12] は [6] で与えられている定義方程式を用いる. 本論文では [8] に基づき, Kummer 曲面をテータ関数を用いて定義した場合でも同様であることを示した. また, 実際に等分多項式を計算するアルゴリズムを構成し, 四則演算の回数での計算量を以下で与えた.

主定理 2. 任意の $m \in \mathbb{Z}_{>1}$ に対して, 等分多項式 μ_m を求めるアルゴリズムの四則演算回数での計算量は $O(m^6(\log m)^2 \log\log m)$ である.

本論文の構成は以下の通りである. 第 2 章では準備として, テータ関数と Kummer 曲面の定義と諸公式を述べる. また, Kummer 曲面と種数 2 の超楕円曲線のヤコビアンとの関係を述べる. 第 3 章では主結果として, 等分多項式の存在を示す. また, 等分多項式の計算アルゴリズムと計算量評価を与える. 第 4 章では具体例として, Kummer 曲面上の点のスカラー倍を等分多項式を用いて計算する.

2 Gaudry による Kummer 曲面上の擬加法及び, Kummer 曲面と種数 2 の超楕円曲線のヤコビアンとの関係

この章では [8] に従って, Gaudry による Kummer 曲面上の擬加法及び, Kummer 曲面と種数 2 の超楕円曲線のヤコビアンとの関係を説明する.

2.1 テータ関数と指標付きテータ関数と諸公式

この節では, Kummer 曲面を定義するために, テータ関数と指標付きテータ関数の定義, さらに導出される諸公式について説明する. 詳細は, [1], [10], [11] を参照せよ.

定義 2.1. $M(2,\mathbb{C})$ を 2 次の複素行列全体とする. このとき, 次数 2 の Siegel 上半空間を

$$\mathcal{H}_2 = \{A \in M(2,\mathbb{C}) \mid A = {}^tA, \mathrm{Im}A > 0\}$$

と定義する.

定義 2.2. $\mathbf{z} \in \mathbb{C}^2, \mathbf{\Omega} \in \mathcal{H}_2$ とする. このとき, Riemann テータ関数を

$$\vartheta(\mathbf{z}, \mathbf{\Omega}) = \sum_{\mathbf{n}\in\mathbb{Z}^2} \exp(\pi i {}^t\mathbf{n}\mathbf{\Omega}\mathbf{n} + 2\pi i {}^t\mathbf{n}\cdot\mathbf{z})$$

と定義する.

$\vartheta(\mathbf{z}, \mathbf{\Omega})$ は絶対収束する.

定義 2.3. $\mathbf{a}, \mathbf{b} \in \mathbb{Q}^2$ とする. このとき, 指標付きテータ関数を

$$\begin{aligned}\vartheta[\mathbf{a};\mathbf{b}](\mathbf{z},\mathbf{\Omega}) &= \sum_{\mathbf{n}\in\mathbb{Z}^2} \exp(\pi i {}^t(\mathbf{n}+\mathbf{a})\mathbf{\Omega}(\mathbf{n}+\mathbf{a}) + 2\pi i {}^t(\mathbf{n}+\mathbf{a})\cdot(\mathbf{z}+\mathbf{b})) \\ &= \exp(\pi i {}^t\mathbf{a}\mathbf{\Omega}\mathbf{a} + 2\pi i {}^t\mathbf{a}\cdot(\mathbf{z}+\mathbf{b}))\cdot\vartheta(\mathbf{z}+\mathbf{\Omega}\mathbf{a}+\mathbf{b},\mathbf{\Omega})\end{aligned}$$

と定義する. さらに, $\mathbf{z} = (0,0)$ での指標付きテータ関数の値をテータ定数と呼ぶ.

以下では, $\mathbf{a}, \mathbf{b} \in \left\{0, \frac{1}{2}\right\}^2$ として, 指標 $[\mathbf{a};\mathbf{b}]$ をみる.

$$\vartheta[\mathbf{a};\mathbf{b}](-\mathbf{z},\mathbf{\Omega}) = (-1)^{4{}^t\mathbf{a}\cdot\mathbf{b}}\vartheta[\mathbf{a};\mathbf{b}](\mathbf{z},\mathbf{\Omega})$$

が成り立ち, 16 個の指標付きテータ関数に番号をつける.

定義 2.4. 10 個の偶関数の指標付きテータ関数を

$$\begin{aligned}
\vartheta_1(\mathbf{z}) &= \vartheta[(0,0);(0,0)](\mathbf{z},\mathbf{\Omega}),\\
\vartheta_2(\mathbf{z}) &= \vartheta\left[(0,0);\left(\frac{1}{2},\frac{1}{2}\right)\right](\mathbf{z},\mathbf{\Omega}),\\
\vartheta_3(\mathbf{z}) &= \vartheta\left[(0,0);\left(\frac{1}{2},0\right)\right](\mathbf{z},\mathbf{\Omega}),\\
\vartheta_4(\mathbf{z}) &= \vartheta\left[(0,0);\left(0,\frac{1}{2}\right)\right](\mathbf{z},\mathbf{\Omega}),\\
\vartheta_5(\mathbf{z}) &= \vartheta\left[\left(\frac{1}{2},0\right);(0,0)\right](\mathbf{z},\mathbf{\Omega}),\\
\vartheta_6(\mathbf{z}) &= \vartheta\left[\left(\frac{1}{2},0\right);\left(0,\frac{1}{2}\right)\right](\mathbf{z},\mathbf{\Omega}),\\
\vartheta_7(\mathbf{z}) &= \vartheta\left[\left(0,\frac{1}{2}\right);(0,0)\right](\mathbf{z},\mathbf{\Omega})),\\
\vartheta_8(\mathbf{z}) &= \vartheta\left[\left(\frac{1}{2},\frac{1}{2}\right);(0,0)\right](\mathbf{z},\mathbf{\Omega}),\\
\vartheta_9(\mathbf{z}) &= \vartheta\left[\left(0,\frac{1}{2}\right);\left(\frac{1}{2},0\right)\right](\mathbf{z},\mathbf{\Omega}),\\
\vartheta_{10}(\mathbf{z}) &= \vartheta\left[\left(\frac{1}{2},\frac{1}{2}\right);\left(\frac{1}{2},\frac{1}{2}\right)\right](\mathbf{z},\mathbf{\Omega})
\end{aligned}$$

と定義し, $\vartheta_1(\mathbf{z}), \vartheta_2(\mathbf{z}), \vartheta_3(\mathbf{z}), \vartheta_4(\mathbf{z})$ を基本テータ関数と呼ぶ. また, 6 個の奇関数の指標付きテータ関数を

$$\begin{aligned}
\vartheta_{11}(\mathbf{z}) &= \vartheta\Big[\Big(0,\frac{1}{2}\Big);\Big(0,\frac{1}{2}\Big)\Big](\mathbf{z},\boldsymbol{\Omega}),\\
\vartheta_{12}(\mathbf{z}) &= \vartheta\Big[\Big(0,\frac{1}{2}\Big);\Big(\frac{1}{2},\frac{1}{2}\Big)\Big](\mathbf{z},\boldsymbol{\Omega}),\\
\vartheta_{13}(\mathbf{z}) &= \vartheta\Big[\Big(\frac{1}{2},0\Big);\Big(\frac{1}{2},0\Big)\Big](\mathbf{z},\boldsymbol{\Omega}),\\
\vartheta_{14}(\mathbf{z}) &= \vartheta\Big[\Big(\frac{1}{2},\frac{1}{2}\Big);\Big(\frac{1}{2},0\Big)\Big](\mathbf{z},\boldsymbol{\Omega}),\\
\vartheta_{15}(\mathbf{z}) &= \vartheta\Big[\Big(\frac{1}{2},0\Big);\Big(\frac{1}{2},\frac{1}{2}\Big)\Big](\mathbf{z},\boldsymbol{\Omega}),\\
\vartheta_{16}(\mathbf{z}) &= \vartheta\Big[\Big(\frac{1}{2},\frac{1}{2}\Big);\Big(0,\frac{1}{2}\Big)\Big](\mathbf{z},\boldsymbol{\Omega})
\end{aligned}$$

と定義する. このとき, $\vartheta_{11}(\mathbf{0}) = \cdots = \vartheta_{16}(\mathbf{0}) = 0$ である. さらに, $2\boldsymbol{\Omega}$ での 4 つの指標付きテータ関数を

$$\begin{aligned}
\Theta_1(\mathbf{z}) &= \vartheta[(0,0);(0,0)](\mathbf{z},2\boldsymbol{\Omega}),\\
\Theta_2(\mathbf{z}) &= \vartheta\Big[\Big(\frac{1}{2},\frac{1}{2}\Big);(0,0)\Big](\mathbf{z},2\boldsymbol{\Omega}),\\
\Theta_3(\mathbf{z}) &= \vartheta\Big[\Big(0,\frac{1}{2}\Big);(0,0)\Big](\mathbf{z},2\boldsymbol{\Omega}),\\
\Theta_4(\mathbf{z}) &= \vartheta\Big[\Big(\frac{1}{2},0\Big);(0,0)\Big](\mathbf{z},2\boldsymbol{\Omega})
\end{aligned}$$

と定義する.

任意の $\mathbf{z} \in \mathbb{C}^2$ について, 以下の 2 倍公式が成り立つ.

$$\begin{aligned}
\vartheta_1(\mathbf{z})\vartheta_1(\mathbf{0}) &= \Theta_1(\mathbf{z})^2 + \Theta_2(\mathbf{z})^2 + \Theta_3(\mathbf{z})^2 + \Theta_4(\mathbf{z})^2,\\
\vartheta_2(\mathbf{z})\vartheta_2(\mathbf{0}) &= \Theta_1(\mathbf{z})^2 + \Theta_2(\mathbf{z})^2 - \Theta_3(\mathbf{z})^2 - \Theta_4(\mathbf{z})^2,\\
\vartheta_3(\mathbf{z})\vartheta_3(\mathbf{0}) &= \Theta_1(\mathbf{z})^2 - \Theta_2(\mathbf{z})^2 + \Theta_3(\mathbf{z})^2 - \Theta_4(\mathbf{z})^2,\\
\vartheta_4(\mathbf{z})\vartheta_4(\mathbf{0}) &= \Theta_1(\mathbf{z})^2 - \Theta_2(\mathbf{z})^2 - \Theta_3(\mathbf{z})^2 + \Theta_4(\mathbf{z})^2.
\end{aligned} \tag{2.1}$$

$$\begin{aligned}
4\Theta_1(2\mathbf{z})\Theta_1(\mathbf{0}) &= \vartheta_1(\mathbf{z})^2 + \vartheta_2(\mathbf{z})^2 + \vartheta_3(\mathbf{z})^2 + \vartheta_4(\mathbf{z})^2,\\
4\Theta_2(2\mathbf{z})\Theta_2(\mathbf{0}) &= \vartheta_1(\mathbf{z})^2 + \vartheta_2(\mathbf{z})^2 - \vartheta_3(\mathbf{z})^2 - \vartheta_4(\mathbf{z})^2,\\
4\Theta_3(2\mathbf{z})\Theta_3(\mathbf{0}) &= \vartheta_1(\mathbf{z})^2 - \vartheta_2(\mathbf{z})^2 + \vartheta_3(\mathbf{z})^2 - \vartheta_4(\mathbf{z})^2,\\
4\Theta_4(2\mathbf{z})\Theta_4(\mathbf{0}) &= \vartheta_1(\mathbf{z})^2 - \vartheta_2(\mathbf{z})^2 - \vartheta_3(\mathbf{z})^2 + \vartheta_4(\mathbf{z})^2.
\end{aligned} \tag{2.2}$$

また、任意の $\mathbf{z}, \mathbf{z}' \in \mathbb{C}^2$ について, 以下の加法公式が成り立つ.

$$\begin{aligned}
\vartheta_1(\mathbf{z}+\mathbf{z}')\vartheta_1(\mathbf{z}-\mathbf{z}') &= \Theta_1(2\mathbf{z})\Theta_1(2\mathbf{z}') + \Theta_2(2\mathbf{z})\Theta_2(2\mathbf{z}') + \Theta_3(2\mathbf{z})\Theta_3(2\mathbf{z}') + \Theta_4(2\mathbf{z})\Theta_4(2\mathbf{z}'),\\
\vartheta_2(\mathbf{z}+\mathbf{z}')\vartheta_2(\mathbf{z}-\mathbf{z}') &= \Theta_1(2\mathbf{z})\Theta_1(2\mathbf{z}') + \Theta_2(2\mathbf{z})\Theta_2(2\mathbf{z}') - \Theta_3(2\mathbf{z})\Theta_3(2\mathbf{z}') - \Theta_4(2\mathbf{z})\Theta_4(2\mathbf{z}'),\\
\vartheta_3(\mathbf{z}+\mathbf{z}')\vartheta_3(\mathbf{z}-\mathbf{z}') &= \Theta_1(2\mathbf{z})\Theta_1(2\mathbf{z}') - \Theta_2(2\mathbf{z})\Theta_2(2\mathbf{z}') + \Theta_3(2\mathbf{z})\Theta_3(2\mathbf{z}') - \Theta_4(2\mathbf{z})\Theta_4(2\mathbf{z}'),\\
\vartheta_4(\mathbf{z}+\mathbf{z}')\vartheta_4(\mathbf{z}-\mathbf{z}') &= \Theta_1(2\mathbf{z})\Theta_1(2\mathbf{z}') - \Theta_2(2\mathbf{z})\Theta_2(2\mathbf{z}') - \Theta_3(2\mathbf{z})\Theta_3(2\mathbf{z}') + \Theta_4(2\mathbf{z})\Theta_4(2\mathbf{z}').
\end{aligned} \tag{2.3}$$

$$\begin{aligned}
4\Theta_1(\mathbf{z}+\mathbf{z}')\Theta_1(\mathbf{z}-\mathbf{z}') &= \vartheta_1(\mathbf{z})\vartheta_1(\mathbf{z}') + \vartheta_2(\mathbf{z})\vartheta_2(\mathbf{z}') + \vartheta_3(\mathbf{z})\vartheta_3(\mathbf{z}') + \vartheta_4(\mathbf{z})\vartheta_4(\mathbf{z}'),\\
4\Theta_2(\mathbf{z}+\mathbf{z}')\Theta_2(\mathbf{z}-\mathbf{z}') &= \vartheta_1(\mathbf{z})\vartheta_1(\mathbf{z}') + \vartheta_2(\mathbf{z})\vartheta_2(\mathbf{z}') - \vartheta_3(\mathbf{z})\vartheta_3(\mathbf{z}') - \vartheta_4(\mathbf{z})\vartheta_4(\mathbf{z}'),\\
4\Theta_3(\mathbf{z}+\mathbf{z}')\Theta_3(\mathbf{z}-\mathbf{z}') &= \vartheta_1(\mathbf{z})\vartheta_1(\mathbf{z}') - \vartheta_2(\mathbf{z})\vartheta_2(\mathbf{z}') + \vartheta_3(\mathbf{z})\vartheta_3(\mathbf{z}') - \vartheta_4(\mathbf{z})\vartheta_4(\mathbf{z}'),\\
4\Theta_4(\mathbf{z}+\mathbf{z}')\Theta_4(\mathbf{z}-\mathbf{z}') &= \vartheta_1(\mathbf{z})\vartheta_1(\mathbf{z}') - \vartheta_2(\mathbf{z})\vartheta_2(\mathbf{z}') - \vartheta_3(\mathbf{z})\vartheta_3(\mathbf{z}') + \vartheta_4(\mathbf{z})\vartheta_4(\mathbf{z}').
\end{aligned} \tag{2.4}$$

さらに, 以下のテータ定数の関係式が成り立つ.

$$\begin{aligned}\vartheta_5(\mathbf{0})^2\vartheta_6(\mathbf{0})^2 &= \vartheta_1(\mathbf{0})^2\vartheta_4(\mathbf{0})^2 - \vartheta_2(\mathbf{0})^2\vartheta_3(\mathbf{0})^2,\\ \vartheta_7(\mathbf{0})^2\vartheta_9(\mathbf{0})^2 &= \vartheta_1(\mathbf{0})^2\vartheta_3(\mathbf{0})^2 - \vartheta_2(\mathbf{0})^2\vartheta_4(\mathbf{0})^2,\\ \vartheta_8(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 &= \vartheta_1(\mathbf{0})^2\vartheta_2(\mathbf{0})^2 - \vartheta_3(\mathbf{0})^2\vartheta_4(\mathbf{0})^2.\end{aligned} \tag{2.5}$$

$$\begin{aligned}\vartheta_5(\mathbf{0})^4 + \vartheta_6(\mathbf{0})^4 &= \vartheta_1(\mathbf{0})^4 - \vartheta_2(\mathbf{0})^4 - \vartheta_3(\mathbf{0})^4 + \vartheta_4(\mathbf{0})^4,\\ \vartheta_7(\mathbf{0})^4 + \vartheta_9(\mathbf{0})^4 &= -\vartheta_1(\mathbf{0})^4 + \vartheta_2(\mathbf{0})^4 - \vartheta_3(\mathbf{0})^4 + \vartheta_4(\mathbf{0})^4,\\ \vartheta_8(\mathbf{0})^4 + \vartheta_{10}(\mathbf{0})^4 &= \vartheta_1(\mathbf{0})^4 + \vartheta_2(\mathbf{0})^4 - \vartheta_3(\mathbf{0})^4 - \vartheta_4(\mathbf{0})^4.\end{aligned} \tag{2.6}$$

2.2 Gaudry による Kummer 曲面上の擬加法

この節では Kummer 曲面の定義, Kummer 曲面上の擬加法について説明する.

定義 2.5. $\mathbf{\Omega} \in \mathcal{H}_2$ とする. $\mathbf{\Omega}$ に付随する Kummer 曲面を

$$\kappa\colon \mathbf{z} \mapsto (\vartheta_1(2\mathbf{z})\colon \vartheta_2(2\mathbf{z})\colon \vartheta_3(2\mathbf{z})\colon \vartheta_4(2\mathbf{z}))$$

により定まる $\mathbb{C}^2$ から $\mathbb{P}^3(\mathbb{C})$ への写像 κ の像と定義する.

ϑ_i は同時に 0 にならない. また, ϑ_i は次の周期性をもつ.

$$\vartheta[(0,0);\mathbf{b}](\mathbf{z}+\mathbf{\Omega m}+\mathbf{n},\mathbf{\Omega}) = \exp(-2\pi i {}^t\mathbf{m}\cdot\mathbf{b} - \pi i {}^t\mathbf{m}\mathbf{\Omega m} - 2\pi i {}^t\mathbf{m}\cdot\mathbf{z})\vartheta[(0,0);\mathbf{b}](\mathbf{z},\mathbf{\Omega}).$$

これより, 格子 $\mathbb{Z}^2 + \mathbf{\Omega}\mathbb{Z}^2$ 分の差がある 2 つのベクトルは写像 κ により同じ点に写される. 従って, 写像 κ は Abel 多様体 $J = \mathbb{C}^2/(\mathbb{Z}^2 + \mathbf{\Omega}\mathbb{Z}^2)$ からの写像とみなせる. $\mathbf{\Omega}$ に付随する Kummer 曲面は 2 次元射影多様体であり, $\mathcal{K}(\mathbf{\Omega})$ または, 単に $\mathcal{K}$ と表す.

κ によって $\mathcal{K}$ 上の群構造を定めることはできない. ϑ_i は偶関数より, 任意の $\mathbf{z} \in J$ に対して, $\kappa(\mathbf{z}) = \kappa(-\mathbf{z})$ である. これより, κ は準同型写像ではない. しかし, $\mathcal{K}$ 上の点に対して, 2 倍と擬加法を定められる. つまり, 未知の $\mathbf{z}, \mathbf{z}' \in J$ に対して, $\kappa(\mathbf{z}), \kappa(\mathbf{z}'), \kappa(\mathbf{z}-\mathbf{z}')$ が既知であれば, 2 倍公式 (2.1), (2.2) を用いて, $\kappa(2\mathbf{z})$, 加法公式 (2.3), (2.4) を用いて, $\kappa(\mathbf{z}+\mathbf{z}')$ を計算できる.

次に、具体的に 2 倍アルゴリズムと擬加法アルゴリズムを作るために, $\mathcal{K}$ の射影方程式をみていく.

$$\begin{aligned}a = \vartheta_1(\mathbf{0}), b = \vartheta_2(\mathbf{0}), c = \vartheta_3(\mathbf{0}), d = \vartheta_4(\mathbf{0}),\\ A = \Theta_1(\mathbf{0}), B = \Theta_2(\mathbf{0}), C = \Theta_3(\mathbf{0}), D = \Theta_4(\mathbf{0})\end{aligned}$$

により, パラメータ化された Kummer 曲面 $\mathcal{K} = \mathcal{K}_{a,b,c,d}$ を考える. 以下の関係式は (2.2) に $\mathbf{z} = \mathbf{0}$ を代入することで得られる.

$$\begin{aligned}4A^2 &= a^2 + b^2 + c^2 + d^2,\\ 4B^2 &= a^2 + b^2 - c^2 - d^2,\\ 4C^2 &= a^2 - b^2 + c^2 - d^2,\\ 4D^2 &= a^2 - b^2 - c^2 + d^2.\end{aligned} \tag{2.7}$$

$\mathcal{K}$ 上の点の射影座標を $(x\colon y\colon z\colon t)$ と書く. すなわち, ある $\mathbf{z} \in \mathbb{C}^2, \lambda \in \mathbb{C}^\times (= \mathbb{C}\backslash\{0\})$ に対して,

$$x = \lambda\vartheta_1(\mathbf{z}), y = \lambda\vartheta_2(\mathbf{z}), z = \lambda\vartheta_3(\mathbf{z}), t = \lambda\vartheta_4(\mathbf{z})$$

とする. $\mathcal{K}$ の射影方程式は以下で与えられる.

$$L \coloneqq x^4+y^4+z^4+t^4+2Exyzt-F(x^2t^2+y^2z^2)-G(x^2z^2+y^2t^2)-H(x^2y^2+z^2t^2)=0.$$

但し,

$$E=\frac{256abcdA^2B^2C^2D^2}{(a^2d^2-b^2c^2)(a^2c^2-b^2d^2)(a^2b^2-c^2d^2)}, \tag{2.8}$$

$$F=\frac{a^4-b^4-c^4+d^4}{a^2d^2-b^2c^2}, \tag{2.9}$$

$$G=\frac{a^4-b^4+c^4-d^4}{a^2c^2-b^2d^2}, \tag{2.10}$$

$$H=\frac{a^4+b^4-c^4-d^4}{a^2b^2-c^2d^2} \tag{2.11}$$

である. E,F,G,H の分母が 0 になるときがある. (2.5) より, E,F,G,H の分母はそれぞれ, $\vartheta_5(\mathbf{0}),...,\vartheta_{10}(\mathbf{0})$ の積で表せる. これより, 条件を設ける.

条件 1. a,b,c,d は 0 ではなく, 他の 6 つの指標付きテータ定数 $\vartheta_5(\mathbf{0}),...,\vartheta_{10}(\mathbf{0})$ も 0 でない.

$\mathcal{K}$ 上の点を 2 倍するときに, 条件 1 のみだと問題が起こる. そのため, 条件 2 を設ける.

条件 2. 条件 1 を満たし, さらに, A,B,C,D も 0 でない.

以下, $\mathcal{K}=\mathcal{K}_{a,b,c,d}$ を条件 2 を満たす Kummer 曲面とする.
L と 2 倍公式 (2.1),(2.2) より, 点の 2 倍アルゴリズムを構成できる.

Algorithm 1 点の 2 倍アルゴリズム : DoubleKummer(P)

Input: $P=(x:y:z:t)\in\mathcal{K}$

Output: $2P=(X:Y:Z:T)\in\mathcal{K}$

1: $x'=\frac{1}{A^2}(x^2+y^2+z^2+t^2)^2$.
2: $y'=\frac{1}{B^2}(x^2+y^2-z^2-t^2)^2$.
3: $z'=\frac{1}{C^2}(x^2-y^2+z^2-t^2)^2$.
4: $t'=\frac{1}{D^2}(x^2-y^2-z^2+t^2)^2$.
5: $X=\frac{1}{a}(x'+y'+z'+t')$.
6: $Y=\frac{1}{b}(x'+y'-z'-t')$.
7: $Z=\frac{1}{c}(x'-y'+z'-t')$.
8: $T=\frac{1}{d}(x'-y'-z'+t')$.
9: **return** $(X:Y:Z:T)$

また,L と加法公式 (2.3), (2.4) より, 点の擬加法アルゴリズムを構成できる.

Algorithm 2 点の擬加法アルゴリズム： PseudoAddKummer(P, Q, R)

Input: $P = (x : y : z : t), Q = (\underline{x} : \underline{y} : \underline{z} : \underline{t}), R = (\bar{x} : \bar{y} : \bar{z} : \bar{t}) \in \mathcal{K}$（但し, R は $P + Q$ と $P - Q$ のどちらか一方の点であり, $\bar{x}\bar{y}\bar{z}\bar{t} \neq 0$）

Output: $P + Q$ と $P - Q$ の内 R とは異なる点 $(X : Y : Z : T) \in \mathcal{K}$

1: $x' = \frac{1}{A^2}(x^2 + y^2 + z^2 + t^2)(\underline{x}^2 + \underline{y}^2 + \underline{z}^2 + \underline{t}^2)$.
2: $y' = \frac{1}{B^2}(x^2 + y^2 - z^2 - t^2)(\underline{x}^2 + \underline{y}^2 - \underline{z}^2 - \underline{t}^2)$.
3: $z' = \frac{1}{C^2}(x^2 - y^2 + z^2 - t^2)(\underline{x}^2 - \underline{y}^2 + \underline{z}^2 - \underline{t}^2)$.
4: $t' = \frac{1}{D^2}(x^2 - y^2 - z^2 + t^2)(\underline{x}^2 - \underline{y}^2 - \underline{z}^2 + \underline{t}^2)$.
5: $X = (x' + y' + z' + t')/\bar{x}$.
6: $Y = (x' + y' - z' - t')/\bar{y}$.
7: $Z = (x' - y' + z' - t')/\bar{z}$.
8: $T = (x' - y' - z' + t')/\bar{t}$.
9: **return** $(X : Y : Z : T)$

さらに, 点の 2 倍アルゴリズムと擬加法アルゴリズムを組み合わせることで, 点のスカラー倍アルゴリズムを構成できる.

Algorithm 3 点のスカラー倍アルゴリズム

Input: $n \in \mathbb{Z}_{>1}$,$P \in \mathcal{K}$（但し, 座標に 0 を持たない.）

Output: $nP \in \mathcal{K}$

1: **if** $n = 2$ **then**
2: **return** DoubleKummer(P).
3: **end if**
4: $n = n_0 2^k + n_1 2^{k-1} + \cdots + n_{k-1} 2 + n_k$（$n_0 = 1, n_i \in \{0, 1\}, k \in \mathbb{N}$）と n を 2 進展開する.
5: $P_n = P$.
6: $P_p =$DoubleKummer(P).
7: **for** $i = 1, ...k$ **do**
8: $Q =$ PseudoAddKummer(P_p, P_m, P).
9: **if** $n_i = 1$ **then**
10: $P_p =$DoubleKummer(P_p).
11: $P_n = Q$.
12: **else**
13: $P_n =$DoubleKummer(P_m).
14: $P_p = Q$.
15: **end if**
16: **end for**
17: **return** P_n

$\mathcal{K} = \mathcal{K}_{a,b,c,d}$ の方程式 L に対して, 次の 16 個の点が $\mathcal{K}$ の結節点である.

$$(a\colon b\colon c\colon d), (a\colon b\colon -c\colon -d), (a\colon -b\colon c\colon -d), (a\colon -b\colon -c\colon d),$$
$$(b\colon a\colon d\colon c), (b\colon a\colon -d\colon -c), (b\colon -a\colon d\colon -c), (b\colon -a\colon -d\colon c),$$
$$(c\colon d\colon a\colon b), (c\colon d\colon -a\colon -b), (c\colon -d\colon a\colon -b), (c\colon -d\colon -a\colon b),$$
$$(d\colon c\colon b\colon a), (d\colon c\colon -b\colon -a), (d\colon -c\colon b\colon -a), (d\colon -c\colon -b\colon a).$$

$\mathcal{K}$ 上の点での擬加法に関する単位元は $(a\colon b\colon c\colon d)$ であり, $(a\colon b\colon c\colon d) = O$ とおく.

2.3 Kummer 曲面と種数 2 の超楕円曲線のヤコビアンとの関係

この節では Kummer 曲面と種数 2 の超楕円曲線のヤコビアンとの関係について説明する.

まず, 曲線の方程式とテータ定数の関係をみる. $\mathcal{C}$ を以下で与えられる $\mathbb{C}$ 上の種数 2 の曲線とし, 右辺は重根を持たないとする.

$$y^2 = f(x) = x(x-1)(x-\alpha)(x-\beta)(x-\gamma).$$

2 つのテータ定数に対して,

$$e = \vartheta_8(\mathbf{0}), f = \vartheta_{10}(\mathbf{0})$$

とおく. このとき,

$$\alpha = \frac{a^2c^2}{b^2d^2}, \beta = \frac{c^2e^2}{d^2f^2}, \gamma = \frac{a^2e^2}{b^2f^2}$$

が成り立つ. (2.5), (2.6) より,

$$e^4 + f^4 = a^4 + b^4 - c^4 - d^4,$$
$$e^2f^2 = a^2b^2 - c^2d^2$$

であるから,

$$e^2 + f^2 = \pm 4AB,$$
$$e^2 - f^2 = \pm 4CD$$

である. 従って,

$$(e^2, f^2) = (2(AB+CD), 2(AB-CD)), (2(AB-CD), 2(AB+CD)),$$
$$(-2(AB-CD), -2(AB+CD)), (-2(AB+CD), -2(AB-CD))$$

が成り立つ. よって,

$$\frac{e^2}{f^2} = \frac{AB+CD}{AB-CD}, \frac{AB-CD}{AB+CD}$$

である. 以上より, 曲線の方程式を基本テータ定数で表すことができる.

次に,Kummer 曲面 $\mathcal{K}$ 上の点を曲線 $\mathcal{C}$ のヤコビアンに写す関数をみる.

補題 2.6. a,b,c,d は条件 2 を満たすとする. このとき, $\vartheta_7(\mathbf{0})^4 \neq \vartheta_9(\mathbf{0})^4, \vartheta_5(\mathbf{0})^4 \neq \vartheta_6(\mathbf{0})^4, \vartheta_8(\mathbf{0})^4 \neq \vartheta_{10}(\mathbf{0})^4$ である.

証明. $\vartheta_8(\mathbf{0})^4 = \vartheta_{10}(\mathbf{0})^4$ と仮定する.

$$\frac{\vartheta_8(\mathbf{0})^2}{\vartheta_{10}(\mathbf{0})^2} = \frac{AB+CD}{AB-CD}$$

とすると,

$$1 = \frac{A^2B^2 + 2ABCD + C^2D^2}{A^2B^2 - 2ABCD + C^2D^2}.$$

これより, $ABCD = 0$ となる. しかし, これは条件 2 に矛盾する.

$$\frac{\vartheta_8(\mathbf{0})^2}{\vartheta_{10}(\mathbf{0})^2} = \frac{AB-CD}{AB+CD}$$

のときも同様である. また, $\vartheta_7(\mathbf{0})^4 \neq \vartheta_9(\mathbf{0})^4, \vartheta_5(\mathbf{0})^4 \neq \vartheta_6(\mathbf{0})^4$ についても同様に成り立つ. □

$\vartheta_5(\mathbf{z})^2, ..., \vartheta_{16}(\mathbf{z})^2$ は以下のように基本テータ関数とテータ定数で表すことができる.

$$\vartheta_5(\mathbf{z})^2 = \frac{\vartheta_3(\mathbf{z})^2\vartheta_8(\mathbf{0})^2\vartheta_9(\mathbf{0})^2 + \vartheta_2(\mathbf{z})^2\vartheta_7(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 - \vartheta_4(\mathbf{z})^2\vartheta_9(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 - \vartheta_1(\mathbf{z})^2\vartheta_7(\mathbf{0})^2\vartheta_8(\mathbf{0})^2}{\vartheta_9(\mathbf{0})^4 - \vartheta_7(\mathbf{0})^4}$$

$$\vartheta_6(\mathbf{z})^2 = \frac{\vartheta_4(\mathbf{z})^2\vartheta_7(\mathbf{0})^2\vartheta_8(\mathbf{0})^2 + \vartheta_1(\mathbf{z})^2\vartheta_9(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 - \vartheta_3(\mathbf{z})^2\vartheta_7(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 - \vartheta_2(\mathbf{z})^2\vartheta_8(\mathbf{0})^2\vartheta_9(\mathbf{0})^2}{\vartheta_7(\mathbf{0})^4 - \vartheta_9(\mathbf{0})^4}$$

$$\vartheta_7(\mathbf{z})^2 = \frac{\vartheta_4(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_8(\mathbf{0})^2 + \vartheta_2(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 - \vartheta_3(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 - \vartheta_1(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_8(\mathbf{0})^2}{\vartheta_6(\mathbf{0})^4 - \vartheta_5(\mathbf{0})^4}$$

$$\vartheta_8(\mathbf{z})^2 = \frac{\vartheta_4(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_7(\mathbf{0})^2 + \vartheta_3(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_9(\mathbf{0})^2 - \vartheta_2(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_9(\mathbf{0})^2 - \vartheta_1(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_7(\mathbf{0})^2}{\vartheta_9(\mathbf{0})^4 - \vartheta_7(\mathbf{0})^4}$$

$$\vartheta_9(\mathbf{z})^2 = \frac{\vartheta_3(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_8(\mathbf{0})^2 + \vartheta_1(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 - \vartheta_4(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 - \vartheta_2(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_8(\mathbf{0})^2}{\vartheta_8(\mathbf{0})^4 - \vartheta_{10}(\mathbf{0})^4}$$

$$\vartheta_{10}(\mathbf{z})^2 = \frac{\vartheta_2(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_7(\mathbf{0})^2 + \vartheta_1(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_9(\mathbf{0})^2 - \vartheta_4(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_9(\mathbf{0})^2 - \vartheta_3(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_7(\mathbf{0})^2}{\vartheta_7(\mathbf{0})^4 - \vartheta_9(\mathbf{0})^4}$$

$$\vartheta_{11}(\mathbf{z})^2 = \frac{\vartheta_3(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 + \vartheta_1(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_8(\mathbf{0})^2 - \vartheta_4(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_8(\mathbf{0})^2 - \vartheta_2(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2}{\vartheta_6(\mathbf{0})^4 - \vartheta_5(\mathbf{0})^4}$$

$$\vartheta_{12}(\mathbf{z})^2 = \frac{\vartheta_4(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 + \vartheta_2(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_8(\mathbf{0})^2 - \vartheta_3(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_8(\mathbf{0})^2 - \vartheta_1(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2}{\vartheta_8(\mathbf{0})^4 - \vartheta_{10}(\mathbf{0})^4}$$

$$\vartheta_{13}(\mathbf{z})^2 = \frac{\vartheta_3(\mathbf{z})^2\vartheta_7(\mathbf{0})^2\vartheta_8(\mathbf{0})^2 + \vartheta_2(\mathbf{z})^2\vartheta_9(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 - \vartheta_4(\mathbf{z})^2\vartheta_7(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 - \vartheta_1(\mathbf{z})^2\vartheta_8(\mathbf{0})^2\vartheta_9(\mathbf{0})^2}{\vartheta_7(\mathbf{0})^4 - \vartheta_9(\mathbf{0})^4}$$

$$\vartheta_{14}(\mathbf{z})^2 = \frac{\vartheta_4(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_9(\mathbf{0})^2 + \vartheta_3(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_7(\mathbf{0})^2 - \vartheta_2(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_7(\mathbf{0})^2 - \vartheta_1(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_9(\mathbf{0})^2}{\vartheta_7(\mathbf{0})^4 - \vartheta_9(\mathbf{0})^4}$$

$$\vartheta_{15}(\mathbf{z})^2 = \frac{\vartheta_3(\mathbf{z})^2\vartheta_9(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2 + \vartheta_2(\mathbf{z})^2\vartheta_7(\mathbf{0})^2\vartheta_8(\mathbf{0})^2 - \vartheta_4(\mathbf{z})^2\vartheta_8(\mathbf{0})^2\vartheta_9(\mathbf{0})^2 - \vartheta_1(\mathbf{z})^2\vartheta_7(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2}{\vartheta_7(\mathbf{0})^4 - \vartheta_9(\mathbf{0})^4}$$

$$\vartheta_{16}(\mathbf{z})^2 = \frac{\vartheta_4(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_7(\mathbf{0})^2 + \vartheta_3(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_9(\mathbf{0})^2 - \vartheta_2(\mathbf{z})^2\vartheta_5(\mathbf{0})^2\vartheta_9(\mathbf{0})^2 - \vartheta_1(\mathbf{z})^2\vartheta_6(\mathbf{0})^2\vartheta_7(\mathbf{0})^2}{\vartheta_7(\mathbf{0})^4 - \vartheta_9(\mathbf{0})^4}.$$

よって, 結節点でない $P = (x : y : z : t) \in \mathcal{K}_{a,b,c,d}$ を与えれば, $\vartheta_5(\mathbf{z})^2, ..., \vartheta_{16}(\mathbf{z})^2$ を計算できる.

以下で, Mumford 表現の定義をする. 詳細は [13] を参照せよ.

定義 2.7. 任意の $P \in J$ に対して,

$$D_P = P_1 + P_2 - 2\infty$$

という形の因子が対応する. 但し, $P_1, P_2 \in \mathcal{C}$ であり, ∞ は無限遠点である. P_1, P_2 が無限遠点でなく, $P_1 = (x_1, y_1), P_2(x_2, y_2), x_1 \neq x_2$ とする. 多項式 $u, v \in \mathbb{C}[x]$ を

$$\begin{aligned} u &= (x - x_1)(x - x_2), \\ v &= \frac{y_1(x - x_2)}{x_1 - x_2} + \frac{y_2(x - x_1)}{x_2 - x_1} \end{aligned}$$

で定義する. 組 (u, v) を P または D_P の Mumford 表現と呼ぶ. P_1, P_2 が上の条件を満たさない場合も Mumford 表現 (u, v) が定まる.

$\vartheta_{16}(\mathbf{z}) \neq 0$ のとき,

$$\begin{aligned} u_0 &= \frac{\alpha\vartheta_8(\mathbf{0})^2\vartheta_{14}(\mathbf{z})^2}{\vartheta_{10}(\mathbf{0})^2\vartheta_{16}(\mathbf{z})^2}, \\ u_1 &= \frac{(\alpha - 1)\vartheta_5(\mathbf{0})^2\vartheta_{13}(\mathbf{z})^2}{\vartheta_{10}(\mathbf{0})^2\vartheta_{16}(\mathbf{z})^2} - u_0 - 1 \end{aligned}$$

と定義する. このとき, $u(x) = u_1x + u_0$ が D_P の Mumford 表現の u 多項式である. $v(x) = v_1x + v_0$ とすると, v_0^2 は以下である.

$$\begin{aligned} v_0^2 =& \frac{-\vartheta_1(\mathbf{0})^4\vartheta_3(\mathbf{0})^4\vartheta_8(\mathbf{0})^2\vartheta_{14}(\mathbf{z})^2}{(\vartheta_2(\mathbf{0})^2\vartheta_4(\mathbf{0})^2\vartheta_{10}(\mathbf{0})^2\vartheta_{16}(\mathbf{z})^2)^3}\Big(\vartheta_2(\mathbf{0})^2\vartheta_3(\mathbf{0})^2\vartheta_9(\mathbf{0})^4\vartheta_7(\mathbf{z})^2\vartheta_{12}(\mathbf{z})^2 + \vartheta_1(\mathbf{0})^2\vartheta_4(\mathbf{0})^2\vartheta_7(\mathbf{0})^4\vartheta_9(\mathbf{z})^2\vartheta_{11}(\mathbf{z})^2 \\ &+ 2\vartheta_1(\mathbf{0})^2\vartheta_2(\mathbf{0})^2\vartheta_3(\mathbf{0})^2\vartheta_4(\mathbf{0})^2(\vartheta_1(\mathbf{z})^2\vartheta_3(\mathbf{z})^2 + \vartheta_2(\mathbf{z})^2\vartheta_4(\mathbf{z})^2) \\ &- 2\vartheta_1(\mathbf{0})\vartheta_2(\mathbf{0})\vartheta_3(\mathbf{0})\vartheta_4(\mathbf{0})\vartheta_1(\mathbf{z})\vartheta_2(\mathbf{z})\vartheta_3(\mathbf{z})\vartheta_4(\mathbf{z})(\vartheta_1(\mathbf{0})^2\vartheta_3(\mathbf{0})^2 + \vartheta_2(\mathbf{0})^2\vartheta_4(\mathbf{0})^2)\Big). \end{aligned}$$

v_1 は $u(x) \mid (v(x)^2 - f(x))$ より, 求められる.

$\vartheta_{16}(\mathbf{z}) = 0$ のときは D_P の Mumford 表現の u 多項式の次数が 2 より小さいときの因子に対応しており,

$$u_0 = \frac{\alpha\vartheta_8(\mathbf{0})^2\vartheta_{14}(\mathbf{z})^2}{(\alpha - 1)\vartheta_5(\mathbf{0})^2\vartheta_{13}(\mathbf{z})^2 - \alpha\vartheta_8(\mathbf{0})^2\vartheta_{14}(\mathbf{z})^2}$$

となる. 因子の Mumford 表現はこのとき, $(x + u_0, \pm\sqrt{f(-u_0)})$ である.

よって, $\mathcal{K}_{a,b,c,d}$ から $\mathcal{C}$ のヤコビアンへの写像を得た. ヤコビアンの因子を $\mathcal{K}$ に写すアルゴリズムを得ることは, 方程式を解くことに還元できる.

2.4 有限体

この節では, 今までの操作を有限体上でも扱えるようにする.

$\mathbb{F}_q$ を標数が奇数である有限体とし, a, b, c, d を条件 2 を満たす $\mathbb{F}_q$ の元とする. $\mathcal{K}_{a,b,c,d}$ に対応する曲線の方程式を得たい. しかし, e^2, f^2 を得るには, 平方根をとる必要がある. そのため, 条件を設ける.

条件 3. a, b, c, d は条件 2 を満す体 k の元である. さらに, (2.7) で定義される $\frac{C^2D^2}{A^2B^2}$ は k で平方である.

以下, $\mathcal{K} = \mathcal{K}_{a,b,c,d}$ を条件 3 を満たす Kummer 曲面とする. [8] によれば, 曲線 $\mathcal{C}$ が通常 (ordinary) であれば点の擬加法アルゴリズムが $\mathbb{F}_q$ 上で正当である. 以下, 曲線 $\mathcal{C}$ が通常であるとする.

3　等分多項式 μ_m

この章では等分多項式 μ_m の存在を示し, 実際に構成する.

3.1　等分多項式 μ_m の存在

この節では等分多項式 μ_m の存在を示す.

k を標数が 0 の体または, 標数が 2 でない有限体とする. $P \in J(\bar{k})$ に対して, $\kappa(P) = (\xi_1(P) \colon \xi_2(P) \colon \xi_3(P) \colon \xi_4(P)) = (x \colon y \colon z \colon t)$ とする. 簡単のため $\xi_i(P)$ を ξ_i と書く. O' を J の単位元とする. このとき, $\kappa(O') = O$ である. J 上の m 倍写像を $[m]$ で表す. $\mathcal{K}$ 上の点の 2 倍写像を $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$ と表す. すなわち, $\kappa([2]P) = \delta(\kappa(P))$ である.2 倍公式 (2.1), (2.2) より, δ_i は係数を k にもつ次数 4 の $\xi_1, \xi_2, \xi_3, \xi_4$ の斉次多項式である. また, 加法公式 (2.3), (2.4) より, 任意の $P, Q \in J(\bar{k}), i = 1, 2, 3, 4$ に対して,

$$\xi_i(P+Q)\xi_i(P-Q) = c' \cdot B_i(\kappa(P), \kappa(Q)) \tag{3.1}$$

となる定数 $c' \in \bar{k}^\times$ が存在するような係数を k にもつ斉次変数の 2 つの組 $(\xi_1(P), ..., \xi_4(P)), (\xi_1(Q), ..., \xi_4(Q))$ の双二次形式である多項式 B_i が存在する.

補題 3.1. L_i を L に $\xi_i = 0$ を代入して得られる多項式とする. このとき, L_i は $k[\xi_1, ..., \xi_{i-1}, \xi_{i+1}, ..., \xi_4]$ で既約である.

証明. $i = 1$ のとき,

$$L_1 = \xi_2^4 + \xi_3^4 + \xi_4^4 - F\xi_2^2\xi_3^2 - G\xi_2^2\xi_4^2 - H\xi_3^2\xi_4^2$$

である. $\mathbb{P}^2$ 内の曲線 $\mathcal{D}$ を

$$\mathcal{D} \colon f(\xi_2 : \xi_3 : \xi_4) = 0$$

とする. [2, 命題 6.3] より $\mathcal{D}$ が非特異ならば, $\mathcal{D}$ は既約である. 従って, $\mathcal{D}$ が特異点を持たないことを云う. まず, L_1 を各変数で偏微分をする.

$$\frac{\partial f}{\partial \xi_2} = 4\xi_2^3 - 2F\xi_2\xi_3^2 - 2G\xi_2\xi_4^2, \tag{3.2}$$

$$\frac{\partial f}{\partial \xi_3} = 4\xi_3^3 - 2F\xi_2^2\xi_3 - 2H\xi_3\xi_4^2, \tag{3.3}$$

$$\frac{\partial f}{\partial \xi_4} = 4\xi_4^3 - 2G\xi_2^2\xi_4 - 2H\xi_3^2\xi_4. \tag{3.4}$$

$\xi_2 = 0$ とする. (3.3) より, $4\xi_3^3 - 2H\xi_3\xi_4^2 = 0$ とする. (3.4) より, $4\xi_4^3 - 2H\xi_3^2\xi_4 = 0$ とする. $\xi_3 = 0$ ならば, $\xi_4 = 0$ であり, $\xi_4 = 0$ ならば, $\xi_3 = 0$ である. 従って, $\xi_3\xi_4 \neq 0$ とする. これより, $(4 - H^2)\xi_3^2 = 0, \xi_4^2 = \frac{H}{2}\xi_3^2$ を得る. よって, $H = \pm 2$ のときのみ, $\mathcal{C}$ は特異点を持つ. 同様にして, $\xi_3 = 0$ とすると, $G = \pm 2$ のときのみ, $\mathcal{C}$ は特異点を持ち, $\xi_4 = 0$ とすると, $F = \pm 2$ のときのみ, $\mathcal{C}$ は特異点を持つ.

次に, $F, G, H \neq \pm 2$ を云う. $H = 2$ と仮定すると, (2.11) より, $a^4 + b^4 - c^4 - d^4 = 2(a^2b^2 - c^2d^2)$. 整理して $a^2 - b^2 = \pm(c^2 - d^2)$ を得る. しかし, これは (2.7) と条件 2 に矛盾する. 次に, $H = -2$ と仮定すると, (2.11) より, $a^4 + b^4 - c^4 - d^4 = -2(a^2b^2 - c^2d^2)$. 整理して $a^2 + b^2 = \pm(c^2 + d^2)$ を得る. しかし, これは

(2.7) と条件 2 に矛盾する. よって, $H \neq \pm 2$ である. 同様にして, $F, G \neq \pm 2$ である. 従って, $\mathcal{C}$ の特異点は座標に 0 を持たない.

よって, (3.2), (3.3), (3.4) を

$$\begin{aligned} 2\xi_2^2 - F\xi_3^2 - G\xi_4^2 &= 0, \\ -F\xi_2^2 + 2\xi_3^2 - H\xi_4^2 &= 0, \\ -G\xi_2^2 - H\xi_3^2 + 2\xi_4^2 &= 0 \end{aligned}$$

とする. これを行列に直すと,

$$\begin{pmatrix} 2 & -F & -G \\ -F & 2 & -H \\ -G & -H & 2 \end{pmatrix} \begin{pmatrix} \xi_2^2 \\ \xi_3^2 \\ \xi_4^2 \end{pmatrix} = \mathbf{0}.$$

行列式を計算する.

$$\begin{aligned} &\det \begin{pmatrix} 2 & -F & -G \\ -F & 2 & -H \\ -G & -H & 2 \end{pmatrix} \\ &= -2(F^2 + G^2 + H^2 + FGH - 4) \\ &= \frac{-2a^2b^2c^2d^2(a^2+b^2+c^2+d^2)^2(a^2+b^2-c^2-d^2)^2(a^2-b^2+c^2-d^2)^2(a^2-b^2-c^2+d^2)^2}{(a^2d^2-b^2c^2)^2(a^2c^2-b^2d^2)^2(a^2b^2-c^2d^2)^2} \\ &= \frac{-2a^2b^2c^2d^2A^2B^2C^2D^2}{(a^2d^2-b^2c^2)^2(a^2c^2-b^2d^2)^2(a^2b^2-c^2d^2)^2} \\ &\neq 0. \end{aligned}$$

従って, $\begin{pmatrix} \xi_2^2 \\ \xi_3^2 \\ \xi_4^2 \end{pmatrix}$ は自明な解しか持たない. よって, $\mathcal{D}$ は特異点を持たない. $i = 2, 3, 4$ のときも同様に従う. □

定義 3.2. イデアル I は, ある $m \in \mathbb{Z}_{\geq 1}$ に対して, $f^m \in I$ ならば, $f \in I$ を満たすとき, 根基イデアルと定義する. また, $I \subset k[x_0, ..., x_n]$ をイデアルとする. 集合

$$\{f \in I \mid \text{ある } m \in \mathbb{Z}_{\geq 1} \text{に対して, } f^m \in I\}$$

を I の根基といい, $\sqrt{I}$ と書く.

補題 3.3. $I = \langle L, \xi_i \rangle$ を L と ξ_i により生成される $k[\xi_1, ..., \xi_4]$ のイデアルとする. このとき, I は素イデアルである. 特に, I は根基イデアルである. すなわち, $\sqrt{I} = I$ である.

証明. $R = k[\xi_1, ..., \xi_4], R_i = k[\xi_1, ..., \xi_{i-1}, 0, \xi_{i+1}, ..., \xi_4]$ とする. 環準同型写像 $\psi_i : R \to R_i$ を

$$\psi_i(g(\xi_1, ..., \xi_4)) \mapsto g(\xi_1, ..., \xi_{i-1}, 0, \xi_{i+1}, ..., \xi_4)$$

で定義する. このとき, $L_i = \psi_i(L)$ である. I_i を L_i で生成される R_i のイデアルとする. このとき, $I = \psi_i^{-1}(I_i)$ である. 補題 3.1 より, I_i は R_i の素イデアルである. よって, I は R の素イデアルである. ゆえに, I は R の根基イデアルである. □

次に [7] に従って, 射影多様体に関する準備をする.

定義 3.4. イデアル $I \subset k[x_0, ..., x_n]$ が各 $f \in I$ に対して, f の斉次成分が I に属しているとき, I は斉次であると定義する.

定義 3.5. k を体とし, $f_1, ..., f_s \in k[x_0, ..., x_n]$ を斉次多項式とする.

$$\mathbf{V}(f_1, ..., f_s) = \{(a_0 : ... : a_n) \in \mathbb{P}^n(k) \mid \text{任意の } 1 \leq i \leq s \text{ に対して, } f_i(a_0, ..., a_n) = 0\}$$

とする. $\mathbf{V}(f_1, ..., f_s)$ を $(f_1, ..., f_s)$ によって定義された射影多様体と呼ぶ.

定義 3.6. 任意の斉次イデアル $I \subset k[x_0, ..., x_n]$ に対して,

$$\mathbf{V}(I) = \{p \in \mathbb{P}^n(k) \mid \text{任意の } f \in I \text{ に対して, } f(p) = 0\}$$

と定義する. このとき, $\mathbf{V}(I)$ は射影多様体である. また, 射影多様体 $V \subset \mathbb{P}^n(k)$ に対して,

$$\mathbf{I}(V) = \{f \in k[x_0, ..., x_n] \mid \text{任意の } (a_0 : ... : a_n) \in V \text{ に対して, } f(a_0, ..., a_n) = 0\}$$

と定義する.

定理 3.7. (射影多様体に対する強零点定理)
k を代数閉体とし, I を $k[x_0, ..., x_n]$ の斉次イデアルとする. $V = \mathbf{V}(I)$ が $\mathbb{P}^n(k)$ の空でない射影多様体ならば, $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ である.

証明. [7, Theorem 9] を参照せよ. □

定義 3.8. 部分集合 $S \subset \mathbb{P}^n$ に対して, Zariski 閉包 $\overline{S}$ を S を含む最小の射影多様体と定義する.

定義 3.9. 射影多様体 $V \subset \mathbb{P}^n$ が既約であることを射影多様体 V_1, V_2 に対し, $V = V_1 \cup V_2$ ならば, $V = V_1$ または $V = V_2$ が成り立つことと定義する.

定義 3.10. V を射影多様体とし, $S \subset V$ とする. $\bar{S} = V$ が成り立つとき, S が V で Zariski 稠密であると定義する.

命題 3.11. 射影多様体 $V, W \subset \mathbb{P}^n$ に対して,

$$V = (V \cap W) \cup \overline{(V \backslash W)}$$

が成り立つ.

証明. V は射影多様体であり, $V \backslash W \subset V$ より, $\overline{V \backslash W} \subset V$ である. また, $V \cap W \subset V$ であるから, $V \supset (V \cap W) \cup \overline{(V \backslash W)}$ である. 逆については $V \backslash W \subset \overline{V \backslash W}$ より, $V \subset (V \cap W) \cup \overline{(V \backslash W)}$ が従う. □

命題 3.12. 射影多様体 V が既約であることは, 任意の $W \subsetneq V$ である射影多様体 W に対して, $V \backslash W$ が V で Zariski 稠密であることと同値である.

証明. V を既約とし, 任意の $W \subsetneq V$ をとる. 命題 3.11 より, $V = W \cup \overline{(V \backslash W)}$ である. V は既約であり,$W \subsetneq V$ より, $V = \overline{V \backslash W}$ である. 逆について, $V_1, V_2 \subset V$ に対して, $V = V_1 \cup V_2$ であるとする. $V_1 \subsetneq V$ ならば, $\overline{V \backslash V_1} = V$ である. また, $V \backslash V_1 \subset V_2$ より, $\overline{V \backslash V_1} \subset V_2$ である. これより, $V \subset V_2$ である. すなわち, $V = V_2$ である. □

定理 3.13. 任意の $m \in \mathbb{Z}_{\geq 0}, i = 1,2,3,4$ に対して, 以下を満たす斉次多項式 $\mu_{m,i} \in k[\xi_1, ..., \xi_4]/\langle L \rangle$ が存在する.

$$\begin{aligned} \mu_{0,1} = a, \mu_{0,2} = b, \mu_{0,3} = c, \mu_{0,4} = d, \\ \mu_{1,i} = \xi_i, \\ \mu_{2m,i} = \delta_i(\mu_m) \quad (m \geq 1), \qquad (3.5) \\ \mu_{2m+1,i}\xi_i = B_i(\mu_{m+1}, \mu_m) \quad (m \geq 1). \qquad (3.6) \end{aligned}$$

但し, $\mu_m = (\mu_{m,1}, \mu_{m,2}, \mu_{m,3}, \mu_{m,4})$ である.
任意の $P \in J(\bar{k})$ に対して,

$$\kappa([m]P) = (\mu_{m,1}(\kappa(P)) : \mu_{m,2}(\kappa(P)) : \mu_{m,3}(\kappa(P)) : \mu_{m,4}(\kappa(P))). \qquad (3.7)$$

証明. 帰納法を用いる. $m = 0, 1$ のときは定義より従う. $m < n$ に対して, 条件を満たす $\mu_{m,i}$ が存在すると仮定する. n が偶数のとき, $\mu_{n,i} = \delta_i(\mu_{\frac{n}{2}})$ で定義すると, (3.5) を満たす. 次に, (3.7) より,

$$\kappa([\frac{n}{2}]P) = (\mu_{\frac{n}{2},1}(\kappa(P)) : \mu_{\frac{n}{2},2}(\kappa(P)) : \mu_{\frac{n}{2},3}(\kappa(P)) : \mu_{\frac{n}{2},4}(\kappa(P))).$$

両辺に δ を施すと,

$$\delta\kappa([\frac{n}{2}]P) = \delta(\mu_{\frac{n}{2},1}(\kappa(P)) : \mu_{\frac{n}{2},2}(\kappa(P)) : \mu_{\frac{n}{2},3}(\kappa(P)) : \mu_{\frac{n}{2},4}(\kappa(P))).$$

よって,

$$\kappa([n]P) = (\mu_{n,1}(\kappa(P)) : \mu_{n,2}(\kappa(P)) : \mu_{n,3}(\kappa(P)) : \mu_{n,4}(\kappa(P))).$$

これより, n が偶数のときは成り立つ. 次に, n が奇数のとき, $n = 2l + 1$ とおく. このとき, 任意の $P \in J(\bar{k})$ に対し,

$$\xi_i([2l+1]P)\xi_i(P) = c' B_i(\kappa([l+1]P), \kappa([l]P))$$

となる $c' \in \bar{k}^\times$ が存在する. $i = 1,2,3,4$ に対し, $g_i \in k[\xi_1, ..., \xi_4]$ を

$$g_i = B_i(\mu_{l+1}, \mu_l)$$

と定義する. つまり, $\xi_i([2l+1]P)\xi_i(P) = c' g_i(\kappa(P))$ である. このとき, $\xi_i(Q) = 0$ なる任意の $Q \in J(\bar{k})$ に対して, $g_i(\kappa(Q)) = 0$ である. 従って, 定理 3.7 より, $g_i \in \sqrt{\langle L, \xi_i \rangle_{\bar{k}}}$ である. 但し, $\langle L, \xi_i \rangle_{\bar{k}}$ は L と ξ_i により生成される $\bar{k}[\xi_1, ..., \xi_4]$ のイデアルである. $g_i \in k[\xi_1, ..., \xi_4]$ より, $g_i \in \sqrt{\langle L, \xi_i \rangle_{\bar{k}}} \cap k[\xi_1, ..., \xi_4] = \sqrt{\langle L, \xi_i \rangle_k}$. 但し, $\langle L, \xi_i \rangle_k$ は L と ξ_i により生成される $k[\xi_1, ..., \xi_4]$ のイデアルである. 補題 3.3 より, $\sqrt{\langle L, \xi_i \rangle_k} = \langle L, \xi_i \rangle_k$ が成り立つ. 従って, ある $g_{1,i}, g_{2,i} \in k[\xi_1, ..., \xi_4]$ に対して,

$$g_i = g_{1,i}\xi_i + g_{2,i}L. \qquad (3.8)$$

となる. $g_{1,i} = \mu_{n+1,i}$ とすれば, (3.6) が成り立つ.

$$\xi_i([2l+1]P)\xi_i(P) = c' \mu_{2l+1,i}(\kappa(P))\xi_i(P)$$

であり, $i=1,2,3,4$ に対して, $\xi_i(P)\neq 0$ ならば,

$$\xi_i([2l+1]P)=c'\mu_{2l+1,i}(\kappa(P)).$$

ゆえに,

$$\begin{aligned}\kappa([2l+1]P)&=(\xi_1([2l+1]P):\xi_2([2l+1]P):\xi_3([2l+1]P):\xi_4([2l+1]P))\\&=(c'\mu_{2l+1,1}(\kappa(P)):c'\mu_{2l+1,2}(\kappa(P)):c'\mu_{2l+1,3}(\kappa(P)):c'\mu_{2l+1,4}(\kappa(P)))\\&=(\mu_{2l+1,1}(\kappa(P)):\mu_{2l+1,2}(\kappa(P)):\mu_{2l+1,3}(\kappa(P)):\mu_{2l+1,4}(\kappa(P)))\end{aligned}\tag{3.9}$$

が成り立つ.

$$\begin{aligned}U&=\{P\in J(\bar{k})\mid i=1,2,3,4\text{ に対して},\xi_i(P)\neq 0\},\\T&=\{P\in J(\bar{k})\mid \kappa([2l+1]P)=(\mu_{2l+1,1}(\kappa(P)),...\mu_{2l+1,4}(\kappa(P)))\}\end{aligned}$$

と定義する. このとき, (3.9) より, $U\subset T$ である. 定義より T は射影多様体である. よって, $\overline{U}\subset T$ である. また, $J(\bar{k})\backslash U$ は射影多様体である. $W=J(\bar{k})\backslash U\subsetneq J(\bar{k})$ とする. J は Abel 多様体であるから, 既約である. 従って, 命題 3.12 より, $J(\bar{k})\backslash W=J(\bar{k})\backslash(J(\bar{k})\backslash U)=U$ は $J(\bar{k})$ で Zariski 稠密である. よって, $\overline{U}=J(\bar{k})$ である. ゆえに, $T=J(\bar{k})$ である. これより, n が奇数のときも成り立つ. □

補足 3.14. $\mu_{2m+1,i}$ は [4] より, Gröbner 基底を使って計算できる. また, 以下の初等的な操作でも計算できる. (3.8) で $g_{2,i}$ は ξ_i を含まないとして良い. h_i を (3.8) の ξ_i に 0 を代入して得られる多項式とする. このとき, $h_i=g_{2,i}L_i$ である. 従って, $g_{2,i}=\frac{h_i}{L_i}$ を計算でき, $g_{1,i}=\frac{g_i-g_{2,i}L}{\xi_i}$ も計算できる.

補題 3.15. 任意の $m\geq 0, i=1,2,3,4$ に対して, $\deg(\mu_{m,i})=m^2$ である.

証明. 帰納法を用いる. $m=0,1$ のときは定義より従う. $m<n$ に対して, $\deg(\mu_{m,i})=m^2$ であると仮定する. n が偶数のとき, $\mu_{n,i}=\delta_i(\mu_{\frac{n}{2}})$ が成り立つ. δ_i は次数 4 の斉次多項式であり, $\deg\mu_{\frac{n}{2},i}=\frac{n^2}{4}$ より, $\deg(\mu_{n,i})=n^2$ が成り立つ. 次に, n が奇数のとき, $n=2l+1$ とおく. $\mu_{2l+1}\xi_i=B_i(\mu_{l+1},\mu_l)$ より,

$$\begin{aligned}\deg(\mu_{2l+1}\xi_i)&=\deg(B_i(\mu_{l+1},\mu_l))\\\deg(\mu_{2l+1})+\deg(\xi_i)&=2(l+1)^2+2l^2\\\deg(\mu_{2l+1})+1&=4l^2+4l+2\\\deg(\mu_{2l+1})&=(2l+1)^2.\end{aligned}$$

□

3.2 等分多項式 μ_m の構成と計算量評価

この節では等分多項式 μ_m を構成し, 計算量を評価する.

2 倍公式 (2.1), (2.2) より, δ を構成できる.

Algorithm 4 2倍アルゴリズム：$\delta(\mu_m)$

Input: $\mu_m = (\mu_{m,1}, \mu_{m,2}, \mu_{m,3}, \mu_{m,4})$

Output: μ_{2m}

$S = \frac{1}{A^2} + \frac{1}{B^2} + \frac{1}{C^2} + \frac{1}{D^2}$.

$T = \frac{1}{A^2} + \frac{1}{B^2} - \frac{1}{C^2} - \frac{1}{D^2}$.

$U = \frac{1}{A^2} - \frac{1}{B^2} + \frac{1}{C^2} - \frac{1}{D^2}$.

$V = \frac{1}{A^2} - \frac{1}{B^2} - \frac{1}{C^2} + \frac{1}{D^2}$.

$M_1 = \mu_{m,1}^4 + \mu_{m,2}^4 + \mu_{m,3}^4 + \mu_{m,4}^4$.

$M_2 = \mu_{m,1}^2\mu_{m,2}^2 + \mu_{m,3}^2\mu_{m,4}^2$.

$M_3 = \mu_{m,1}^2\mu_{m,3}^2 + \mu_{m,2}^2\mu_{m,4}^2$.

$M_4 = \mu_{m,1}^2\mu_{m,4}^2 + \mu_{m,2}^2\mu_{m,3}^2$.

$\mu_{2m,1} = \frac{1}{a}(SM_1 + 2TM_2 + 2UM_3 + 2VM_4)$.

$\mu_{2m,2} = \frac{1}{b}(TM_1 + 2SM_2 + 2VM_3 + 2UM_4)$.

$\mu_{2m,3} = \frac{1}{c}(UM_1 + 2VM_2 + 2SM_3 + 2TM_4)$.

$\mu_{2m,4} = \frac{1}{d}(VM_1 + 2UM_2 + 2TM_3 + 2SM_4)$.

return $(\mu_{2m,1}, \mu_{2m,2}, \mu_{2m,3}, \mu_{2m,4})$

アルゴリズム 4 はアルゴリズム 1 を展開したものである.

また, 加法公式 (2.3), (2.4), 補足 3.14 より, 擬加法アルゴリズムを構成できる.

Algorithm 5 擬加法アルゴリズム : $\eta(\mu_{m+1}, \mu_m)$

Input: μ_{m+1}, μ_m

Output: μ_{2m+1}

1: $S = \frac{1}{A^2} + \frac{1}{B^2} + \frac{1}{C^2} + \frac{1}{D^2}$.
2: $T = \frac{1}{A^2} + \frac{1}{B^2} - \frac{1}{C^2} - \frac{1}{D^2}$.
3: $U = \frac{1}{A^2} - \frac{1}{B^2} + \frac{1}{C^2} - \frac{1}{D^2}$.
4: $V = \frac{1}{A^2} - \frac{1}{B^2} - \frac{1}{C^2} + \frac{1}{D^2}$.
5: $N_1 = \mu_{m+1,1}^2\mu_{m,1}^2 + \mu_{m+1,2}^2\mu_{m,2}^2 + \mu_{m+1,3}^2\mu_{m,3}^2 + \mu_{m+1,4}^2\mu_{m,4}^2$.
6: $N_2 = \mu_{m+1,1}^2\mu_{m,2}^2 + \mu_{m+1,2}^2\mu_{m,1}^2 + \mu_{m+1,3}^2\mu_{m,4}^2 + \mu_{m+1,4}^2\mu_{m,3}^2$.
7: $N_3 = \mu_{m+1,1}^2\mu_{m,3}^2 + \mu_{m+1,2}^2\mu_{m,4}^2 + \mu_{m+1,3}^2\mu_{m,1}^2 + \mu_{m+1,4}^2\mu_{m,2}^2$.
8: $N_4 = \mu_{m+1,1}^2\mu_{m,4}^2 + \mu_{m+1,2}^2\mu_{m,3}^2 + \mu_{m+1,3}^2\mu_{m,2}^2 + \mu_{m+1,4}^2\mu_{m,1}^2$.
9: $g_1 = SN_1 + TN_2 + UN_3 + VN_4$.
10: $g_2 = TN_1 + SN_2 + VN_3 + UN_4$.
11: $g_3 = UN_1 + VN_2 + SN_3 + TN_4$.
12: $g_4 = VN_1 + UN_2 + TN_3 + SN_4$.
13: **for** $i = 1, ..., 4$ **do**
14: $\quad h_i = g_i(\xi_1, ..., \xi_{i-1}, 0, \xi_{i+1}, ..., \xi_4)$.
15: $\quad L_i = L(\xi_1, ..., \xi_{i-1}, 0, \xi_{i+1}, ..., \xi_4)$.
16: $\quad \mu_{2m+1,i} = (g_i - (h_i/L_i)L)/\xi_i$.
17: **end for**
18: **return** $(\mu_{2m+1,1}, \mu_{2m+1,2}, \mu_{2m+1,3}, \mu_{2m+1,4})$

アルゴリズム 5 のステップ 13 まではアルゴリズム 2 を展開したものである.

さらに, 2 倍アルゴリズムと擬加法アルゴリズムを組み合わせることで, スカラー倍アルゴリズムを作れる.

Algorithm 6 スカラー倍アルゴリズム

Input: $m \in \mathbb{Z}_{>1}$

Output: μ_m

1: **if** $m = 2$ **then**
2: **return** $\delta(\mu_1)$.
3: **end if**
4: $m = m_0 2^k + m_1 2^{k-1} + \cdots + m_{k-1} 2 + m_k$（$m_0 = 1, n_i \in \{0, 1\}, k \in \mathbb{N}$）と m を 2 進展開する.
5: $\mu_m = \mu_1$.
6: $\mu_p = \delta(\mu_1)$.
7: **for** $i = 1, ...k$ **do**
8: $\nu = \eta(\mu_p, \mu_m)$.
9: **if** $m_i = 1$ **then**
10: $\mu_p = \delta(\mu_p)$.
11: $\mu_m = \nu$.
12: **else**
13: $\mu_m = \delta(\mu_m)$.
14: $\mu_p = \nu$.
15: **end if**
16: **end for**
17: **return** μ_m

アルゴリズムの計算量を k の四則演算の回数で評価する. $\mathbb{A}$ を単位元をもつ任意の可換環とする. $M(n)$ を 2 つの $\mathbb{A}$ 係数 1 変数 n 次多項式の乗算に必要な $\mathbb{A}$ の演算回数とする. このとき, [5] より, $M(n) = O(n \log n \log\log n)$ ととれる. 任意の多項式 $f \in \mathbb{A}[z_1, ..., z_n]$ に対して, $d_{f,j} = \deg_{z_j} f + 1$ と定義し, $d_f = d_{f,1} \cdots d_{f,n}$ と定義する. [9] より, 任意の多項式 $f, g \in \mathbb{A}$ に対して, 積 $h = fg$ は以下の Kronecker 代入を用いて計算できる.

$$\begin{aligned} K_{d_h} :&\mathbb{A}[z_1, ..., z_n] \longrightarrow \mathbb{A}[x], \\ &f \longmapsto f(x, x^{d_{h1}}, x^{d_{h,1}d_{h,2}}, ..., x^{d_{h,1}\cdots d_{h,n-1}}). \end{aligned}$$

とし, $h = K_{d_h}^{-1}(K_{d_h}(f)K_{d_h}(g))$ を計算すればよい.

命題 3.16. 積 $h = fg$ は $M(d_h)$ 回の $\mathbb{A}$ における演算で計算できる.

証明. [9, Proposition 2] を参照せよ. □

アルゴリズム 4 について, $\mu_{m,i}$ は 4 変数 m^2 次斉次多項式である. $\mu_{m,i}$ に対して, $\xi_4 = 1$ と非斉次化し, 3 変数 m^2 次多項式にしたものを $\mu'_{m,i}$ とする. このとき, $1 \leq i, j \leq 4$ に対して, $d_{\mu'^2_{m,i}\mu'^2_{m,j}} = (4m^2+1)^3$ である. 従って, 命題 3.16 より, $\mu'^2_{m,i}\mu'^2_{m,j}$ の計算量は $O(m^6 \log m \log\log m)$ である. 他の計算は定数の乗除であるから問題ない. よって, アルゴリズム 4 の計算量は $O(m^6 \log m \log\log m)$ である.

アルゴリズム 5 について, $1 \leq i, j \leq 4$ に対して, $d_{\mu'^2_{m+1,i}\mu'^2_{m,j}} = ((2m+1)^2+2)^3$ である. 従って, 命題 3.16 より, $\mu'^2_{m+1,i}\mu'^2_{m,i}$ の計算量は $O(m^6 \log m \log\log m)$ である. g_i, h_i, L, L_i に対して, 非斉次化したものをそれぞれ, g'_i, h'_i, L', L'_i とする.h'_i は 2 変数 $\{(2m+1)^2+1\}$ 次多項式であり, 項数は ${}_3H_{\{(2m+1)^2+1\}} = 2(4m^4+8m^3+11m^2+7m+3)$ 項である. L'_i は 2 変数 4 次多項式であり, 項数は 6 項である. よって, h'_i/L'_i の計算量は $O(m^4)$ である. また, L' は 3 変数 4 次多項式であり, 11 項であるから, $(h'_i/L'_i)L'$ の計算量は $O(m^4)$ である. g'_i は 3 変数 $\{(2m+1)^2+1\}$ 次多項式より, $g'_i - (h'_i/L'_i)L'$ の計算量も $O(m^4)$ である. ξ_i での割り算は指数を一つずらすだけである. 他の計算は定数の乗除であるから問題ない. よって, $(g'_i - (h'_i/L'_i)L')/\xi_i$ の計算量は $O(m^4)$ である. よって, アルゴリズム 5 の計算量は $O(m^6 \log m \log\log m)$ である.

アルゴリズム 6 の繰り返し回数は $\lfloor \log_2 m \rfloor$ 回である. 従って, 以下の定理を得る.

定理 3.17. 任意の $m \in \mathbb{Z}_{>1}$ に対して, 等分多項式 μ_m を求めるアルゴリズム 6 の k の四則演算回数での計算量は $O(m^6(\log m)^2 \log\log m)$ である.

4 具体例

$\mathbb{F}_{17}$ 上の種数 2 の曲線 $\mathcal{C}$ を

$$y^2 = x(x-1)(x-2)(x-3)(x-10)$$

ととる. このとき, $\frac{e^2}{f^2} = 7$ とすると, $O = (a\colon b\colon c\colon d) = (4\colon 1\colon 8\colon 6)$ と選べる. これより, $\mathcal{K}$ の射影方程式は以下である.

$$L \coloneqq x^4+y^4+z^4+t^4+2xyzt+6(x^2t^2+y^2z^2)-6(x^2z^2+y^2t^2)+5(x^2y^2+z^2t^2) = 0.$$

このとき, $\mu_2 = (\mu_{2,1}, \mu_{2,2}, \mu_{2,3}, \mu_{2,4}), \mu_3 = (\mu_{3,1}, \mu_{3,2}, \mu_{3,3}, \mu_{3,4})$ は以下である.

$$\begin{aligned}
\mu_{2,1} &= 2(x^4+y^4+z^4+y^4) + 13(x^2y^2+z^2t^2) + 7(x^2z^2+y^2t^2) + 14(x^2t^2+y^2z^2),\\
\mu_{2,2} &= 9(x^4+y^4+z^4+y^4) + 16(x^2y^2+z^2t^2) + 5(x^2z^2+y^2t^2) + 11(x^2t^2+y^2z^2),\\
\mu_{2,3} &= 6(x^4+y^4+z^4+y^4) + 7(x^2y^2+z^2t^2) + 2(x^2z^2+y^2t^2) + 15(x^2t^2+y^2z^2),\\
\mu_{2,4} &= 16(x^4+y^4+z^4+y^4) + 16(x^2y^2+z^2t^2) + 3(x^2z^2+y^2t^2) + 14(x^2t^2+y^2z^2).
\end{aligned}$$

$$\begin{aligned}
\mu_{3,1} = {} & x^9 + (-4y^2-2z^2+2t^2)x^7 + (4y^4+6y^2z^2-z^4-6y^2t^2-2z^2t^2-t^4)x^5\\
& + (4y^6-5y^4z^2+3y^2z^4+z^6+5y^4t^2+y^2z^2t^2+8z^4t^2+3y^2t^4-8z^2t^4-t^6)x^3\\
& + (6y^8-6y^6z^2-4y^4z^4-5y^2z^6-8z^8+6y^6t^2+y^4z^2t^2+2y^2z^4t^2+4z^6t^2\\
& - 4y^4t^4-2y^2z^2t^4-7z^4t^4+5y^2t^6+4z^2t^6-8t^8)x\\
& + 5y^7zt + (7z^3t-7zt^3)y^5 + (3z^5t-6z^3t^3+3zt^5)y^3 + (-6z^7t-7z^5t^3+7z^3t^5+6zt^7)y,\\
\mu_{3,2} = {} & y^9 + (-4x^2+2z^2-2t^2)y^7 + (4x^4-6x^2z^2-z^4+6x^2t^2-2z^2t^2-t^4)y^5\\
& + (4x^6+5x^4z^2+3x^2z^4-z^6-5x^4t^2+x^2z^2t^2-8z^4t^2+3x^2t^4+8z^2t^4+t^6)y^3\\
& + (6x^8+6x^6z^2-4x^4z^4+5x^2z^6-8z^8-6x^6t^2+x^4z^2t^2-2x^2z^4t^2+4z^6t^2\\
& - 4x^4t^4+2x^2z^2t^4-7z^4t^4-5x^2t^6+4z^2t^6-8t^8)y\\
& + 6xz^7t + (3x^3t+7xt^3)z^5 + (-7x^5t-6x^3t^3-7xt^5)z^3 + (5x^7t+7x^5t^3+3x^3t^5-6xt^7)z,\\
\mu_{3,3} = {} & z^9 + (-2x^2+2y^2-4t^2)z^7 + (-x^4-2x^2y^2-y^4+6x^2t^2-6y^2t^2+4t^4)z^5\\
& + (x^6+8x^4y^2-8x^2y^4-y^6+3x^4t^2+x^2y^2t^2+3y^4t^2-5x^2t^4+5y^2t^4+4t^6)z^3\\
& + (-8x^8+4x^6y^2-7x^4y^4+4x^2y^6-8y^8-5x^6t^2+2x^4y^2t^2-2x^2y^4t^2+5y^6t^2\\
& - 4x^4t^4+x^2y^2t^4-4y^4t^4-6x^2t^6+6y^2t^6+6t^8)z\\
& + 5xyt^7 + (7x^3y-7xy^3)t^5 + (3x^5y-6x^3y^3+3xy^5)t^3 + (-6x^7y-7x^5y^3+7x^3y^5+6xy^7)t,\\
\mu_{3,4} = {} & t^9 + (2x^2-2y^2-4z^2)t^7 + (-x^4-2x^2y^2-y^4-6x^2z^2+6y^2z^2+4z^4)t^5\\
& + (-x^6-8x^4y^2+8x^2y^4+y^6+3x^4z^2+x^2y^2z^2+3y^4z^2+5x^2z^4-5y^2z^4+4z^6)t^3\\
& + (-8x^8+4x^6y^2-7x^4y^4+4x^2y^6-8y^8+5x^6z^2-2x^4y^2z^2+2x^2y^4z^2-5y^6z^2\\
& - 4x^4z^4+x^2y^2z^4-4y^4z^4+6x^2z^6-6y^2z^6+6z^8)t\\
& + 6x^7yz + (7y^3z+3yz^3)x^5 + (-7y^5z-6y^3z^3-7yz^5)x^3 + (-6y^7z+3y^5z^3+7y^3z^5+5yz^7)x.
\end{aligned}$$

$\mu_4 = \delta(\mu_2)$ も計算でき, $P = (5\colon 3\colon 4\colon 11) \in \mathcal{K}$ とすると, $2P = (1\colon 13\colon 2\colon 10), 3P = (12\colon 14\colon 13\colon 6), 4P = O$ である.

5 謝辞

本研究は, 著者が首都大学東京大学院理工学研究科数理情報科学専攻博士前期課程在学中に, 同大学院理工学研究科数理情報科学専攻の内田幸寛准教授の指導のもとに行ったものである. 適切な助言を賜り, 熱心に指導してくださった内田幸寛准教授に深く感謝いたします. そしてご多忙の中, 本論文の副査を快諾していただきました内山成憲教授と徳永浩雄教授に深く感謝いたします. また, 2 年間多くの苦楽を共にした髙田尚樹氏や, 今まで支えていただいた家族にも深く感謝いたします.

参考文献

[1] 大西良博，Abel 函数論，中央大学数学教室講究録 6，http://ir.c.chuo-u.ac.jp/repository/search/binary/p/4118/s/2343/，2013.

[2] 難波誠，代数曲線の幾何学，現代数学社，京都，1991.

[3] 松尾和人，超楕円曲線暗号と位数計算，情報セキュリティ総合科学　第 2 巻，pp. 43-61，2010.

[4] T. Becker and V. Weispfenning，Gröbner Bases，Grad. Texts in Math. 141，Springer，New York，1993.

[5] D. G. Cantor and E. Kaltofen，On fast multiplication of polynomials over arbitrary algebras，Acta Inform. 28 (1991)， no. 7， pp. 693-701.

[6] J. W. S. Cassels and E. V. Flynn，Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2，Cambridge Univ.Press，Cambridge，1996.

[7] D. Cox, J. Litlte and D. O'Shea，Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra，4th ed.，Springer，Cham，2015

[8] P. Gaudry，Fast genus 2 arithmetic based on Theta functions，J. Math. Cryptol. 1(2007)，no. 3，pp. 243–265.

[9] J. van der Hoeven and G. Lecerf，On the bit-complexity of sparse polynomial and series multiplication，J. Symbolic Comput. 50(2013)，pp. 227–254 .

[10] D. Mumford，Tata Lectures on Theta I，Progress in Mathematics 28. Birkhäuser，Boston，1983.

[11] D. Mumford，Tata Lectures on Theta II，Progress in Mathematics 43. Birkhäuser，Boston，1984.

[12] Y. Uchida，Canonical local heights and multipulication formulas for the Jacobians of curves of genus 2，Acta Arith. 149(2011)，pp. 111–130.

[13] L. C. Washington，Elliptic Curves: Number Theory and Cryptography，2nd ed.，Chapman & Hall/CRC，Boca Raton，2008.